(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 September 2002 (26.09.2002)

PCT

(10) International Publication Number
WO 02/076062 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/JP02/02394

(22) International Filing Date: 14 March 2002 (14.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2001-076507 16 March 2001 (16.03.2001) JP
2001-199977 29 June 2001 (29.06.2001) JP

(71) Applicant *(for all designated States except US)*: **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.** [JP/JP]; 1006, Oaza Kadoma, Kadoma-shi, Osaka 571-8501 (JP).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KOKADO, Takeshi** [JP/JP]; 5-4-5, Osumigaoka, Kyotanabe-shi, Kyoto 610-0351 (JP). **OKADA, Yasunori** [JP/JP]; 2-38-10, Shodaimotomachi, Hirakata-shi, Osaka 573-1133 (JP). **KUBOTA, Kouji** [JP/JP]; 3-36-402, Ikutamateramachi, Tennoji-ku, Osaka-shi, Osaka 543-0073 (JP). **SAITOU, Takahiro** [JP/JP]; 1645-120, Kusatsu-cho, Kusatsu-shi, Shiga 525-0036 (JP). **ISHIKAWA, Hirokazu** [JP/JP]; 2-27-4, Higashitanabe, Higashisumiyoshi-ku, Osaka-shi, Osaka 546-0032 (JP).

(74) Agent: **OGASAWARA, Shiro**; Daisan-Longev' Bldg., 3-11, Enokicho, Suita-shi, Osaka 564-0053 (JP).

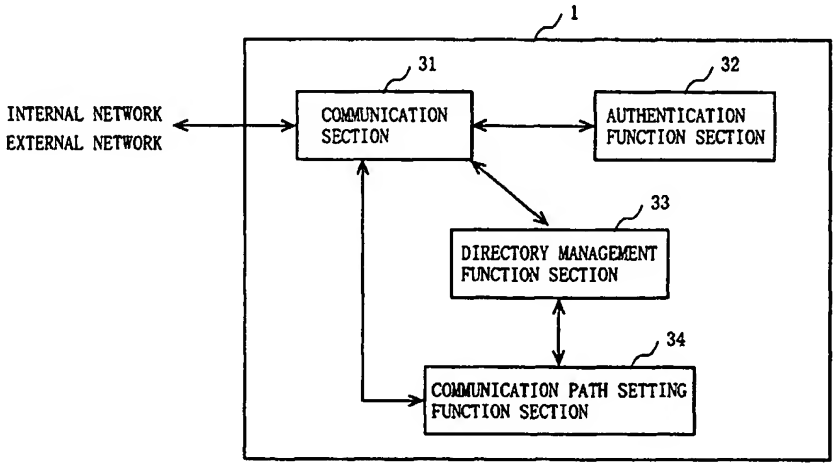
(81) Designated States *(national)*: CN, IN, KR, SG, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR SETTING UP A FIREWALL



(57) Abstract: The home gateway HGW (1) includes a communication section (31), an authentication function section (32), a directory management function section (33), and a communication path setting function section (34). The communication section (31) receives data transmitted to the HGW (1). The authentication function section (32) authenticates the aforementioned data to be from an authorized user or not. Responsive to a service registration, the directory management function section (33) registers service information, checks the matching between the service information and service permission policies, and requests the communication path setting function section (34) to set a communication path. The communication path setting function section (34) monitors the state of data communication along the communication paths, and closes any unnecessary communication paths that may have been set. As a result, it becomes possible to restrict the users who are entitled to accessing each terminal on an internal network from an external network, and to allow a user to access a selected terminal on an internal network.

used for an internal network, referred to as a local address (Local Address: hereinafter abbreviated as "LA"), is not valid for external networks. Therefore, through address conversion technique, an IP address is converted to a global address (Global Address: hereinafter abbreviated as "GA"), which is valid for an external network. An improved version of this address conversion technique is called IP masquerade (Masquerade). According to the IP masquerade technique, communication port numbers of TCP/UDP, a higher-level protocol, are identified. Based on the management of the correspondence between LA's and GA's, it becomes possible for a plurality of LA's to simultaneously communicate based on a single GA.

A network address conversion method which supports a plurality of terminals on an internal network, such that a GA can be shared in the aforementioned manner, is disclosed in Japanese Patent Laid-Open Publication No. 2000-59430. This method aims to allow a terminal on an internal network to communicate with a terminal which is connected to an external network, without requiring conversion of port numbers. According to this method, an internal table indicating address conversion rules is provided in an address conversion apparatus. The internal table stores the correspondence between: pairs (LP, IA) each consisting of a port number (LP) used for communication by a terminal on an internal network and an IP address (IA) of a terminal on an external network; and IP addresses (LA) of terminals on the internal

network. Therefore, in accordance with this address conversion apparatus, based on the setting of the above-mentioned internal table, it is possible to restrict the external network terminals which are entitled to accessing each internal network terminal. By introducing such an address conversion method in a fire wall apparatus, a security measure is realized which restricts the external network terminals which are entitled to accessing each internal network terminal.

On the other hand, in a situation where various devices are interconnected over networks, a user may desire, by manipulating a device which is connected to one network, to obtain service information (e.g., control information or state information) of a device which is connected to another network, in order to control the latter device based on the obtained service information. However, in terms of network security, it would be undesirable to make all of the service information provided on the network available, and the devices associated with such service information controllable, to every user on the network.

As a solution to this problem, Japanese Patent Laid-Open Publication No. 11-275074 discloses a conventional network service management method in which information of different services is provided to different users on the network. According to this network service management method, when providing information occurring on a network to a user, it is ensured that different contents are provided depending on the status of the

to a telephone circuit network, for example, the IA's which are used for distinguishing the terminal apparatuses on the external network do not have fixed values but are subject to changes; therefore, the aforementioned internal table needs to be reorganized every time the IA's are changed. However, such reorganization is very cumbersome, making the address conversion for non-fixed value IA's difficult.

Accordingly, an object of the present invention is to provide a method and apparatus for setting a fire wall which can restrict the users who are entitled to accessing each terminal on an internal network from an external network, and which allows a user to access a selected terminal on an internal network.

On the other hand, according to the above-described device controlling method, when a new component element (a user, a service, etc.) is added to a network, it becomes necessary to set the items which can be allowed to be provided from the new component element to the network. In the case of a home network, for example, a user who is not very familiar with network management may have to take care of such setting when connecting a device to a network. If the items to be allowed to be provided to the network are not well-selected, unrestricted access to such items can occur from outside of the house. Such situations are not desirable in terms of network security.

Accordingly, another object of the present invention is to provide an apparatus and method which, when a new component

element is added to a network, sets preferable access restrictions responsive to a mere connection of the device, thereby providing sufficient security.

DISCLOSURE OF THE INVENTION

To achieve the above objects, the present invention has the following aspects.

A first aspect of the present invention is directed to a fire wall apparatus for preventing unauthorized external access to an internal network having a plurality of servers which are coupled to an external terminal via an external network, wherein each of the plurality of servers provides a service, comprising:

a data processing section for processing communication data which is transmitted from the external terminal and setting a communication path between at least one of the plurality of servers and the external terminal based on the communication data, wherein the communication data at least comprises an external address of the external terminal and user identification data for identifying a user of the external terminal; and

a switching section for connecting the at least one server and the external terminal based on the communication path which is set by the data processing section,

wherein the data processing section includes:

a plurality of function sections; and

a communication section for receiving at least the

communication data and requesting the plurality of function sections to perform processing based on the contents of the data,

wherein the plurality of function sections comprise:

an authentication function section for authenticating the user identification data;

a directory management function section for registering units of service information, where each unit of service information represents an internal address of one of the plurality of servers and a service type in association with predetermined permitted-recipient data designating an external user who is entitled to connecting to the server, and allowing a user who is given authentication by the authentication function section to select one of the units of service information whose permitted-recipient data designates the user; and

a communication path setting function section for setting the communication path using the internal address of the server represented by the unit of service information selected by means of the directory management function section and the external address of the external terminal.

Thus, according to the first aspect, limited external users are entitled to external accessing. After confirming user authentication, the external address of an external terminal used by a particular external user is acquired, and a communication path is set based on the acquired external address. As a result, a service provided on an internal network can be permitted for

access by limited external users who are entitled to external accessing. Even if the external terminal used by the external user is altered, or if the external address of the external terminal used by the external user is changed, similar access can still be realized. When requesting a communication path to be set, the external user can selectively access an accessible service, and even if the same service is being provided by a plurality of servers on the internal network, the external user can access a selected one of such servers. On the other hand, it is possible to designate external users who are entitled to connecting a server on the internal network on a service-to-service basis. Therefore, the security level for each server can be easily adjusted by designating different external users who are entitled to accessing a plurality of servers providing the same service on an internal network.

According to a second aspect based on the first aspect, each unit of service information registered in the directory management function section is registered based on service data at least comprising the internal address and the service type, wherein the service data is transmitted from the server.

Thus, according to the second aspect, the service(s) to be permitted for access from an external network can be registered or altered in accordance with an instruction from a server which is connected to an internal network.

According to a third aspect based on the second aspect, the

service data further comprises service deletion data indicating that the service provided by the server is unavailable, and

wherein each unit of service information registered in the directory management function section is deletable based on the service deletion data.

Thus, according to the third aspect, it is possible to instruct from a server on an internal network whether or not to permit each service on the server for access from an external network.

According to a fourth aspect based on the second aspect, the service data further comprises permitted-recipient alteration data for altering the permitted-recipient data, and

wherein an external user who is entitled to connecting to a service, as designated in each unit of service information registered in the directory management function section, is alterable based on the permitted-recipient alteration data.

Thus, according to the fourth aspect, from an internal network, it is possible to alter or designate external users who are entitled to accessing a service provided on the server.

According to a fifth aspect based on the second aspect, the service data further comprises server identification information for identifying the server in a fixed manner, and

wherein the directory management function section updates each unit of service information with respect to the internal address based on the server identification information.

Thus, according to the fifth aspect, when the internal address of a server on an internal network is altered, it is still possible to associate the server with the altered internal address by recognizing a fixed value which identifies the server. As a result, the alteration of a table which is necessary for internal address conversion can be automatically processed.

According to a sixth aspect based on the first aspect, each unit of service information registered in the directory management function section is registered based on service data at least comprising the internal address and the service type, wherein the service data is acquired from the server by the directory management function section.

Thus, according to the sixth aspect, a service to be permitted for access from an external network can be registered or altered without an instruction from a server which is connected to an internal network.

According to a seventh aspect based on the first aspect, the directory management function section registers each unit of service information based on service data at least comprising the internal address and the service type, and

wherein, if no permitted-recipient data is registered in association with the internal address of one of the plurality of servers and the service type in the directory management function section, the directory management function section automatically generates permitted-recipient data for the service data.

service type in the directory management function section, the directory management function section selects from among the currently registered permitted-recipient data those permitted-recipient data which match a set of conditions stipulated in the service data except for one or more of the conditions, and newly generates the permitted-recipient data for the service data based on the selected permitted-recipient data.

Thus, according to the ninth aspect, if no corresponding permitted-recipient data is present, preferable permitted-recipient data can be generated on permitted-recipient data which is already registered.

According to a tenth aspect based on the seventh aspect, the directory management function section comprises preset permitted-recipient data storage means for storing preset permitted-recipient data to be applied if no permitted-recipient data is registered in association with the internal address of one of the plurality of servers and the service type, and

wherein, if no permitted-recipient data is registered in association with the internal address of one of the plurality of servers and the service type in the directory management function section, the directory management function section selects from among the currently registered permitted-recipient data those permitted-recipient data which match a set of conditions stipulated in the service data except for one or more of the conditions, and

defined for each service which can be permitted for access from an external network. Since a communication path is temporarily set only while the service is valid, and since the communication path is dedicated to each service, further enhanced security can be provided.

According to a twelfth aspect based on the first aspect, the communication path setting function section monitors data transmitted through the communication path having been set, and closes the communication path if no data is transmitted through the communication path in a predetermined period.

Thus, according to the twelfth aspect, even after setting a communication path for a service which can be permitted for access from an external network, if the communication path is not used by external users during a period which is previously set with respect to that service, the communication path is closed. Thus, further enhanced security can be provided.

According to a thirteenth aspect based on the first aspect, the communication path setting function section closes the communication path upon receiving service communication termination data transmitted from the external terminal, wherein the service communication termination data indicates termination of a service communication with the server.

According to a fourteenth aspect based on the first aspect, the communication path setting function section closes the communication path upon receiving service communication

a plurality of function sections; and

a communication section for receiving at least the service data and requesting the plurality of function sections to perform processing based on the contents of the data,

wherein the plurality of function sections comprise:

a directory management function section for registering units of service information, where each unit of service information represents the internal address and the service type in association with predetermined permitted-recipient data designating at least one of the plurality of external terminals which is entitled to connecting to the server; and

a communication path setting function section for, when the service information is registered, setting the communication path using the external address of at least one of the plurality of external terminals designated by the permitted-recipient data and the internal address of the server.

Thus, according to the fifteenth aspect, when service information is registered in the directory management function section based on an instruction from a server, a communication path to the designated permitted recipient can be set even in the absence of communication data from an external terminal.

According to a sixteenth aspect based on the fifteenth aspect, the permitted-recipient data registered in the directory management function section designate all of the plurality of

external terminals to be entitled to connecting to the server.

Thus, according to the sixteenth aspect, a service provided by a server on an internal network can be permitted for access by the external terminals without limitation.

A seventeenth aspect of the present invention is directed to a fire wall setting method for preventing unauthorized external access to an internal network having a plurality of servers which are coupled to an external terminal via an external network, wherein each of the plurality of servers provides a service, comprising:

a data processing step of processing communication data which is transmitted from the external terminal and setting a communication path between at least one of the plurality of servers and the external terminal based on the communication data, wherein the communication data at least comprises an external address of the external terminal and user identification data for identifying a user of the external terminal; and

a connection step of connecting the at least one server and the external terminal based on the communication path which is set by the data processing step,

wherein the data processing step includes:

a communication step of receiving at least the communication data and requesting a plurality of steps to perform processing based on the contents of the data,

wherein the plurality of steps comprise:

an authentication step of authenticating the user identification data;

a directory management step of registering units of service information, where each unit of service information represents an internal address of one of the plurality of servers and a service type in association with predetermined permitted-recipient data designating an external user who is entitled to connecting to the server, and allowing a user who is given authentication by the authentication step to select one of the units of service information whose permitted-recipient data designates the user; and

a communication path setting step of setting the communication path using the internal address of the server represented by the unit of service information selected by means of the directory management step and the external address of the external terminal.

According to an eighteenth aspect based on the seventeenth aspect, each unit of service information registered in the directory management step is registered based on service data at least comprising the internal address and the service type, wherein the service data is transmitted from the server.

According to a nineteenth aspect based on the eighteenth aspect, the service data further comprises service deletion data indicating that the service provided by the server is unavailable, and

wherein each unit of service information registered in the directory management step is deletable based on the service deletion data.

According to a twentieth aspect based on the eighteenth aspect, the service data further comprises permitted-recipient alteration data for altering the permitted-recipient data, and

wherein an external user who is entitled to connecting to a service, as designated in each unit of service information registered in the directory management step, is alterable based on the permitted-recipient alteration data.

According to a twenty-first aspect based on the eighteenth aspect, the service data further comprises server identification information for identifying the server in a fixed manner, and

wherein the directory management step updates each unit of service information with respect to the internal address based on the server identification information.

According to a twenty-second aspect based on the seventeenth aspect, each unit of service information registered in the directory management step is registered based on service data at least comprising the internal address and the service type, wherein the service data is acquired from the server by the directory management step.

According to a twenty-third aspect based on the seventeenth aspect, the directory management step registers each unit of service information based on service data at least comprising the

internal address and the service type, and

wherein, if no permitted-recipient data is registered in association with the internal address of one of the plurality of servers and the service type in the directory management step, the directory management step automatically generates permitted-recipient data for the service data.

According to a twenty-fourth aspect based on the twenty-third aspect, the directory management step comprises a preset permitted-recipient data storage step of storing preset permitted-recipient data to be applied if no permitted-recipient data is registered in association with the internal address of one of the plurality of servers and the service type, and

wherein, if no permitted-recipient data is registered in association with the internal address of one of the plurality of servers and the service type in the directory management step, the directory management step newly generates the permitted-recipient data for the service data based on the preset permitted-recipient data.

According to a twenty-fifth aspect based on the twenty-third aspect, if no permitted-recipient data is registered in association with the internal address of one of the plurality of servers and the service type in the directory management step, the directory management step selects from among the currently registered permitted-recipient data those permitted-recipient data which match a set of conditions stipulated in the service

data except for one or more of the conditions, and newly generates the permitted-recipient data for the service data based on the selected permitted-recipient data.

According to a twenty-sixth aspect based on the twenty-third aspect, the directory management step comprises a preset permitted-recipient data storage step of storing preset permitted-recipient data to be applied if no permitted-recipient data is registered in association with the internal address of one of the plurality of servers and the service type, and

wherein, if no permitted-recipient data is registered in association with the internal address of one of the plurality of servers and the service type in the directory management step, the directory management step selects from among the currently registered permitted-recipient data those permitted-recipient data which match a set of conditions stipulated in the service data except for one or more of the conditions, and

a) newly generates the permitted-recipient data for the service data based on the selected permitted-recipient data if the number of selected permitted-recipient data is equal to or greater than a predetermined value; or

b) newly generates the permitted-recipient data for the service data based on the preset permitted-recipient data if the number of selected permitted-recipient data is smaller than the predetermined value.

According to a twenty-seventh aspect based on the

service, comprising:

a data processing step of processing communication data containing service data which is transmitted from at least one of the plurality of servers and setting a communication path between the server and at least one of the plurality of external terminals based on the communication data, wherein the service data at least comprises an internal address of the server and a service type; and

a connection step of connecting the server and the external terminal based on the communication path which is set by the data processing step,

wherein the data processing step includes:

a communication step of receiving at least the service data and requesting a plurality of steps to perform processing based on the contents of the data,

wherein the plurality of steps comprise:

a directory management step of registering units of service information, where each unit of service information represents the internal address and the service type in association with predetermined permitted-recipient data designating at least one of the plurality of external terminals which is entitled to connecting to the server; and

a communication path setting step of, when the service information is registered, setting the communication path using the external address of at least one of the plurality of external

communication apparatus 100.

FIG. 19 shows an operation sequence of the communication apparatus 100 in the case where a controlled device 151 is newly connected to an IEEE1394 bus 170.

FIG. 20 shows an exemplary displayed image of a control menu acquired by a controlling terminal 141 from the communication apparatus 100.

FIG. 21 shows examples of restriction entries which may be stored in a restriction entry management section 130 of the communication apparatus 100.

FIG. 22 shows other examples of restriction entries which may be stored in a restriction entry management section 130 of the communication apparatus 100.

FIG. 23 illustrates an operation sequence of the communication apparatus 100 in the case where a control menu is requested from a controlling terminal 141.

FIG. 24 shows exemplary preset restriction entries which may be registered in a preset restriction entry storage section 132 of the communication apparatus 100.

FIG. 25 is a flowchart illustrating the operation of a restriction entry generation section 131 of the communication apparatus 100.

FIG. 26 shows an exemplary displayed image of a control menu acquired by a controlling terminal 141 from the communication apparatus 100.

FIG. 27 illustrates the structure of a communication apparatus 1000 according to a third embodiment of the present invention, as well as networks and devices connected thereto.

FIG. 28 illustrates an operation sequence of the communication apparatus 1000 in the case where a controlled device 151 is newly connected to an IEEE1394 bus 170.

FIG. 29 shows an example of information which may be stored in a network information storage section 123 of the communication apparatus 1000.

FIG. 30 illustrates an operation sequence of the communication apparatus 1000 in the case where a control menu is requested from a controlling terminal 141.

FIG. 31 shows examples of restriction entries which may be stored in an individual restriction entry storage section 133 of the communication apparatus 1000.

FIG. 32 is a flowchart illustrating the operation of a restriction entry generation section 131 of the communication apparatus 1000.

FIG. 33 shows an exemplary displayed image of a control menu acquired by a controlling terminal 141 from the communication apparatus 1000.

FIG. 34 shows an exemplary displayed image of a control menu acquired by a controlling terminal 141 from the communication apparatus 1000.

FIG. 35 illustrates the structure of a communication

apparatus 1800 according to a fourth embodiment of the present invention, as well as networks and devices connected thereto.

FIG. 36 illustrates an operation sequence of the communication apparatus 1800 in the case where a controlled device 151 is newly connected to an IEEE1394 bus 170.

FIG. 37 shows an example of information which may be stored in a network information storage section 123 of the communication apparatus 1800.

FIG. 38 illustrates an operation sequence of the communication apparatus 1800 in the case where a control menu is requested from a controlling terminal phone 141, particularly in the case where the number of matching restriction entries is smaller than three.

FIG. 39 shows examples of restriction entries which may be stored in an individual restriction entry storage section 133 of the communication apparatus 1800.

FIG. 40 shows examples of preset restriction entries which may be stored in a preset restriction entry storage section 132 of the communication apparatus 1800.

FIG. 41 illustrates an operation sequence of the communication apparatus 1800 in the case where a control menu is requested from a controlling terminal phone 141, particularly in the case where the number of matching restriction entries is equal to or greater than three.

FIG. 42 is a flowchart illustrating the operation of a

apparatus 2700.

FIG. 51 shows the overall configuration of a network according to a conventional network service management system.

FIG. 52 shows the network information which is provided to a network administrator under a conventional network service management system.

FIG. 53 shows network information which is provided to a service administrator under a conventional network service management system.

FIG. 54 shows network information which is provided to a user of a user terminal under a conventional network service management system.

BEST MODE FOR CARRYING OUT THE INVENTION

Hereinafter, various embodiments of the present invention will be described with reference to the figures.

(first embodiment)

FIG. 1 is a diagram illustrating the fundamental structure of a fire wall apparatus according to a first embodiment of the present invention. Hereinafter, the present embodiment will be described with reference to FIG. 1.

As shown in FIG. 1, according to the present embodiment, a plurality of servers 2-1 to 2-n are coupled to a home gateway apparatus (hereinafter abbreviated as "HGW") 1 via bus connection, thereby creating a LAN as an internal network. As an external

network, a plurality of external terminals 3 are coupled to the HGW 1 via the Internet. Any internal terminals other than the servers 2-1 to 2-n may also be coupled to the internal network, and any external servers other than the external terminals 3 may also be coupled to the external network.

The HGW 1 has a global IP address (GA) assigned thereto, which is used for the purpose of transmission/reception with an external network. Moreover, the HGW 1 performs transmission/reception of packets by using a plurality of port numbers (GP). Each of the servers 2-1 to 2-n has a uniquely assigned local IP address (LA) 1 to n, respectively. Moreover, each of the servers 2-1 to 2-n has port numbers (LP) 1 to n, which respectively correspond to different services provided by that server, for receiving communications from a client terminal. Each external terminal 3 has assigned thereto a global IP address (IA) used for the purpose of transmission/reception with an external network and a port number (IP) employed for such transmission/reception.

Next, the fundamental structure of the internal hardware of the HGW 1 above will be described. FIG. 2 is a block diagram illustrating the fundamental structure of the internal hardware of the HGW 1 according to the present embodiment. Hereinafter, the HGW 1 will be described with reference to FIG. 2.

As shown in FIG. 2, the HGW 1 comprises a CPU 10, a memory 11, and an IP switching section 20. The IP switching section 20

includes: a controller 21, a memory 22, an IP filter function section 23, a forwarding function section 24, an address conversion function section 25, and PHY/MAC (Physical Layer Protocol/Media Access Control) function sections 26a and 26b. The CPU 10 controls the respective function sections and performs processing to transmitted or received data. The memory 11 stores operation programs, data, and the like for the HGW 1. The controller 21 receives setting information from the CPU 10, and sets the IP filter function section 23, the forwarding function section 24, and the address conversion function section 25 based on the setting information. The PHY/MAC function sections 26 perform data transmission/reception to or from an external network or an internal network. The controller 21 instructs the IP filter function section 23, the forwarding function section 24, and the address conversion function section 25 to process data which is received by the PHY/MAC function sections 26. The memory 22 temporarily stores packet data which has been received by the PHY/MAC function sections 26. The IP filter function section 23, which has an internal register for storing a filtering condition, checks the packet data stored in the memory 22 based on the filtering condition stored in the register. If given packet data fails to satisfy the filtering condition, the IP filter function section 23 destroys that packet data. The forwarding function section 24, which has an internal register for storing forwarding information, determines which PHY/MAC function section 26 to

information and service permission policies (the details of which will be described later), and requests the communication path setting function section 34 to set a communication path as necessary. The communication path setting function section 34 sets the IP filter function section 23, the forwarding function section 24, the address conversion function section 25, an application GW (gateway), and the like, and sets a communication path. The communication path setting function section 34 monitors the state of data communication along the communication paths, and closes any unnecessary communication paths that may have been set.

Once the present fire wall apparatus sets a communication path in the switching section 20 of the HGW 1, an external terminal 3 on an external network and a server 2 on an internal network become capable of connecting to each other, so that a service on the server 2 is permitted for access from an external network. The services which are provided on the server 2 on the internal network and which can be permitted for access are managed in the form of service information (the details of which will be described later), and communication paths are set based on this service information. In accordance with the present fire wall apparatus, either "authentication free" services (which do not require authentication of an external user), "permitted after authentication" services (which require authentication of an external user), or "non-permitted" services (which are not

permitted for access from any external networks) can be set as a mode of permission. As for the above-defined "authentication free" service, a communication path is set as soon as the service is registered in the service information, so that any user becomes entitled to access from an external network. As for the above-defined "permitted after authentication" service, a communication path is temporarily set when an authorized user desires access to that service, so that only authorized users are entitled to access. Each of the aforementioned services which can be permitted for access has a validity term, and after the validity term is over, is deleted from the service information. Hereinafter, each of the aforementioned communication path setting processes will be described.

First, the service information setting process and the communication path setting process for "authentication free" services, which are performed in the HGW 1, will be described. FIGS. 4 and 5 are flowcharts illustrating the operation of a communication path setting process performed in the HGW 1. FIGS. 8 to 10 show information tables which are generated and used during the communication path setting process performed in the HGW 1. Hereinafter, with reference to FIGS. 4, 5, and 8 to 10, the communication path setting process will be described.

Referring to FIG. 4, the HGW 1 receives a service registration from a server 2 for registering a service which is compliant with SMTP (Simple Mail Transfer Protocol), FTP (File

Transfer Protocol), or HTTP (Hyper Text Transfer Protocol), etc., in the directory management function section 33 (step S101).

Although the present example illustrates the case where a server 2 makes a service registration to the HGW 1, the present invention is not limited thereto; alternatively, the HGW 1 may acquire service information from a server 2. In that case, the directory management function section 33 executes a process shown in FIG. 13 instead of step S101 in FIG. 4. Specifically, the directory management function section 33 first scans for ports on a server 2 connected to an internal network to search for any ports which are being used by the server 2 (S201). If a port being used by the server is a port which is predetermined under the service specifications (i.e., a so-called "well-known port"), it is certain that a service corresponding to that port is being provided by the server (S202). If a port being used by a server is not a well-known port, the service being provided by the server can be detected by confirming a reply message to the port scan. Examples of methods for the HGW 1 to know that a new server has been connected include detection upon the assignment of a new IP address by DHCP (Dynamic Host Configuration Protocol) and detection through monitoring the MAC address of an ARP (Address Resolution Protocol) packet. In the case of using a network which is designed to be capable of detecting the connection of a new device, as in the case of IPover1394, the HGW 1 detects the connection of a new device by utilizing the mechanism of the

a communication path is set in the switching section 20 of the HGW 1. In the case of a service which is permitted for access by limited users or terminals that are entitled to externally accessing, the user names of such users as well as the IA's and IP's of the external terminals 3 are indicated as the currently permitted recipients. A "service validity term" represents a remainder of the permission validity term of each service type, which is previously set for each service type. A "state" represents whether a given service is currently available or not. Note that, when services are registered in the service information, any service which has the same service type as an existing service but has different server identification information therefrom will be processed as a new service, rather than being regarded as already registered. In other words, services which are supported by each server 2 are registered in the service information on a server to server basis.

If step S102 determines that a pair consisting of a service type and server identification information of the service which is subjected to the aforementioned service registration has not been registered in the service information, the HGW 1 sets detailed service permission policies, based on basic service permission policies which are previously set in the directory management function section 33 (step S109).

FIG. 9 shows exemplary basic service permission policies which may be previously set in the directory management function

section 33. FIG. 10 shows exemplary detailed service permission policies which may be set in the directory management function section 33. The basic service permission policies comprise a permitted recipient, a permission condition, and a permitted port, which are previously set in the directory management function section 33 as conditions for being entitled to externally accessing each service type. As the permitted recipient(s), one or more user names are set in the case where permission is directed to limited users who are entitled to externally accessing; or in the case where permission is directed to limited external terminals 3 which are entitled to connecting, the IA(s) of one or more terminals are set. If the permission condition is "authentication free" and the permitted recipient is "permitted to all", the service is meant to be accessible to any external users, and therefore a communication path is set in the switching section 20 as soon as the service is registered in the service information. If the permission condition is "authentication free" and the permitted recipient is the IA of an external terminal 3, a communication path is set in the switching section 20 once the service is registered in the service information. On the other hand, if the permission condition is "permitted after authentication", a communication path is temporarily set in the switching section 20 when a user who is registered as a permitted recipient user wishes to access the service. At step S109, based on the above-described basic permission policies, the

to step S116. On the other hand, if the permitted port is designated, the HGW 1 determines whether the designated port (GP) is available or not (step S114). If the designated GP is available, the HGW 1 acquires that GP (step S115), and proceeds to step S116. Next, the HGW 1 refers to the service information to determine whether the state of the service is "available" or not (step S116). If the state is "unavailable", the flow is ended. If the state is "available" and the permitted recipient is "permitted to all", the HGW 1 acquires the internal address information (LA and LP) and the address information for external permission (GA of the HGW 1 and GP above) with respect to the service of interest, and sets the IP filter function section 23 and the address conversion function section 25, thereby setting a communication path in the switching section 20 (step S117); thereafter, the flow is ended. If step S117 determines that the state is "available" and the permitted recipient is the IA of an external terminal 3, the HGW 1 acquires the internal address information (LA and LP), the address information for external permission (GA of the HGW 1 and GP above) and the address information of the external terminal 3 (IA and IP of external terminal 3) with respect to the service of interest, and sets the IP filter function section 23 and the address conversion function section 25, thereby setting a communication path in the switching section 20.

On the other hand, if it is determined at step S114 that the designated GP is unavailable, the HGW 1 refers to the service

whether the designated port (GP) is available or not (step S311). If the designated GP is available, the HGW 1 acquires that GP (step S312), and thereafter acquires the internal address information (LA and LP), the address information for external permission (GA of the HGW 1 and GP above) with respect to the authentication-requiring service, and address information of the external terminal 3 (IA and IP of the external terminal 3), and sets the IP filter function section 23 and the address conversion function section 25, thereby temporarily setting a communication path in the switching section 20 (step S313). Then, the HGW 1 adds the aforementioned user name and the address information of the permitted recipient (IA and IP of the external terminal 3) as a currently permitted recipient of the service information (step S315). The address information of the external terminal 3 may be obtained by acquiring an IP address of the transmission source of the communication path setting request data, or may be newly designated by the above user.

Thus, services which are "permitted after authentication" can only be accessed by authorized users. After the user authentication, a communication path is set in the switching section 20 based on the address information of the external terminal 3 currently used by the user. Thereafter, the HGW 1 notifies to the external terminal 3 a port number to be used for the communication with the server 2 to which a communication path is set (step S314), and ends the flow. On the other hand, if it

is determined at step S311 that the designated GP is unavailable, the HGW 1 refers to the service information and sets the state of the authentication-requiring service to "unavailable" (step S316), notifies to the external terminal 3 that the service of interest is unavailable, and ends the flow.

The communication path which is set to the user in the aforementioned manner is temporarily set with respect to the service of interest. The communication path setting function section 34 of the HGW 1 monitors the amount of data communication along the data communication path, and if no data communication is detected in a predetermined period, deletes the communication path. The monitoring of the data communication amount may be carried out in the switching section 20, and the result may be notified to the communication path setting function section 34. Furthermore, the HGW 1 may delete the communication path upon receiving a notification from the external terminal 3 or the server 2 used by the user that the access to the service has been completed.

Next, the service validity term management performed by the HGW 1 will be described. FIG. 7 is a flowchart illustrating the operation of the service validity term management performed by the HGW 1. Hereinafter, the service validity term management will be described with reference to FIG. 7.

Referring to FIG. 7, the HGW 1 determines whether each service that is registered in the service information has a

remaining service validity term or not (step S401). If there is any remaining service validity term, the HGW 1 ends the flow, and keeps checking service validity terms. On the other hand, if the service validity term of a service has expired, the HGW 1 sets the state in the service information to "unavailable" with respect to that service (step S402). Then, the HGW 1 deletes the communication path which is set in the switching section 2 (step S403) and the currently permitted recipient in the service information, with respect to this service (step S404). Next, with respect to this service, the HGW 1 starts an entry deletion timer T (step S405), and observes a predetermined deletion wait period (step S406). If the above-described service registration is performed during this waiting period and re-setting of a service validity term occurs with respect to the above service, the HGW 1 ends the flow (step S407). Thus, by observing a deletion wait period, it is ensured that external access using the same port number (GP) will become possible once the state becomes available again. On the other hand, if the entry deletion timer T overruns the deletion wait period, the HGW 1 deletes the above service from among the entries in the service information (step S408), and ends the flow. Thus, once the service validity term expires, the service is deleted from the service information following the aforementioned deletion wait period.

Next, the operation in which the switching section 20 is set with respect to the communication path which is set in the

aforementioned manner will be described. Firstly, it is assumed in the present embodiment that the IP filter function section 23 and the address conversion function section 25 are set in such a manner that a dynamic IP masquerade is automatically applied to the communications from an internal network to an external network, so that communications are enabled without requiring the directory management function section 33 to set a communication path in the switching section 20. FIG. 11 illustrates information pertaining to a packet filter which is set in the IP filter function section 23 for permitting communications from an internal network to an external network.

In FIG. 11, any direction refers to a direction in which the PHY/MAC function section 26 transmits data. "Outward" indicates a packet which is to be received by the PHY/MAC function section 26b connected to an internal network and transmitted from the PHY/MAC function section 26a connected to an external network. "Inward" indicates a packet which is to be received by the PHY/MAC function section 26a connected to an external network, and transmitted from the PHY/MAC function section 26b connected to an internal network. "SA" (source address) and "DA" (destination address) represent a transmission source address and a receiving destination address, respectively, which are assigned to a packet. "SP" (source port) and "DP" (destination port) represent a port number of the transmission source and a port number of the receiving destination, respectively, which are assigned to a

packet. "ACK" (Acknowledgement Flag) indicates whether an ACK check is to be made or not. An ACK is not set in a packet used for establishing connection, but rather is set in subsequent packets. The information which is set in the IP filter function section 23 is preset as either default setting A or B. When a packet for commencing communications is transmitted from a server 2 on an internal network to the HGW 1, the packet is permitted to pass through the packet filter according to default setting A. A response packet from an external terminal 3 on an external network to the HGW 1 is permitted to pass through the packet filter according to default setting B. On the other hand, when a packet for commencing communications is transmitted from an external terminal 3 on an external network to the HGW 1, the packet is not permitted to pass through according to default setting B, because no ACK is set in this packet. In other words, communications cannot be commenced from an external network to an internal network unless a new packet filter setting is added.

Next, the information which is set in the IP filter function section 23 and the address conversion function section 25 of the switching section 20 will be described with respect to the case where an FTP service is permitted for access from an external network. FIG. 12(a) shows a communication sequence for an FTP service. FIG. 12(b) illustrates an address conversion table which is set in the address conversion function section 25 by the directory management function section 33. FIG. 12(c)

illustrates a packet filter which is set in the IP filter function section 23 by the directory management function section 33. Hereinafter, with reference to FIG. 12, the manner in which packets in a control-related session are transferred in the case where a communication path setting request for an FTP service is made will be described.

First, a packet having assigned therewith a source address IA, a source port number IP1, a destination address GA, and a destination port number 21 is transmitted from an external terminal 3. Next, the HGW 1 receives the packet, and converts the destination address GA and the destination port number 21 to an LA and an LP21 for the FTP server 2, respectively, by applying condition C in the address conversion table of the address conversion function section 25. Thereafter, the IP filter function section 23 performs a filtering process for the packet by applying condition E of the packet filter, whereby the passage of the packet is permitted. Next, the forwarding function section 24 transmits the packet to the FTP server 2 via the PHY/MAC function section 26b which is connected to an internal network.

After receiving the packet from the external terminal 3, the FTP server 2 transmits to the HGW 1 a response packet having assigned therewith a source address LA, a source port number 21, a destination address IA, and a destination port number IP1. Having received the response packet, the HGW 1 performs a filtering process for the response packet by applying default

setting A of the packet filter in the IP filter function section 23, whereby the passage of the response packet is permitted. Thereafter, by applying condition D in the address conversion table of the address conversion function section 25, the source address LA and the source port number 21 are converted to a GA and GP21 for the HGW 1, respectively. Next, the forwarding function section 24 transmits the response packet to the external terminal 3 via the PHY/MAC function section 26a which is connected to an external network.

In the case of the above FTP service, not only the aforementioned control-related session but also a data-related session is established between the external terminal 3 and the FTP server 2 by using a port number 20. Since the data-related session is established by commencing communications from the FTP server 2, communications from an internal network are enabled based on dynamic IP masquerade and the default filtering setting, without requiring a special setting by means of the directory management function section 33.

In the manner of transfer according to the aforementioned FTP service, the IP filter function section 23 and the address conversion function section 25 are set in such a manner that dynamic IP masquerade is automatically applied to the communications from the internal network to the external network, so that communications from the internal network are enabled without requiring the directory management function section 33

to set the switching section 20. However, in order to provide an even higher level of security for the HGW 1, the setting of the dynamic IP masquerade or the default packet filter can be omitted. In that case, in order for an external terminal 3 on an external network to access the FTP server 2, a number of settings must be made for the address conversion suitable for an LP of the FTP server 2 and the packet filter. By providing a template (which supports LP) for a number of settings depending on the service type, the settings for the IP filter function section 23 and the address conversion function section 25 can be easily made. In the case where no such template for setting purposes is provided for the service type of a service which has been registered, a template for setting purposes may be acquired from the server 2 or a predetermined server on the external network to enable setting of the IP filter function section 23 and the address conversion function section 25.

Although the present embodiment illustrates the internal network as one network, a plurality of internal networks may be connected to the HGW 1. This can be achieved by adding a third PHY/MAC function section 26 in the switching section 20, and connecting to the third PHY/MAC function section 26 a second internal network (DMZ: DeMilitarized Zone) embracing servers which may be permitted for access from an external network. Thus, the present invention can provide an enhanced level of security in such cases.

Although the present embodiment illustrates the case where validity term timeout information or registration information from a server is utilized for the transition of the service state from "available" to "unavailable" or from "unavailable" to "available", or for the registration or deletion of service information, the present invention is not limited thereto. Alternatively, the HGW 1 may perform a port scan for the server and, on the basis of changes in the open ports on the server, carry out the transition of the service state or the registration or deletion of service information. Similarly, PING (packet internet groper) may be employed instead of a port scan.

Although the present embodiment illustrates an example where access to the server 2 on the internet work is made from an external network, such access may be made from another device on the internal network. This can be realized by adding detailed service permission policies for a device on the internal network as a currently permitted recipient, or providing another table for permitted recipients. Thus, the security level can be varied depending on whether access is made from an internal location or from an external location, thereby introducing increased convenience.

When generating detailed service permission policies for a given server, an external agent, e.g., the manufacturer of the server may be accessed, and initial values of the detailed service permission policies may be acquired therefrom. As a result, the

manufacture is able to alter the detailed service permission policies stored in that server even after shipment of the server.

As described above, according to the present fire wall apparatus, limited users are permitted to be entitled to externally accessing. After user authentication is confirmed, the address information (IA, IP) of an external terminal used by the user is acquired, and a communication path is set based on the address information. As a result, a service on an internal network can be permitted for access by limited users who are entitled to accessing externally, and a communication path can be set only during a period for which the user requests permission of the service. Access can be similarly made even if the external terminal used by the user is changed, or the IA of the external terminal used by the user is changed. When the user requests for a communication path to be set, the user can selectively access services which are accessible, and even if the same service is provided by a plurality of servers on an internal network, the user can selectively access a relevant server. On the other hand, users who are entitled to accessing a server on an internal network can be designated for each service provided by the server. Therefore, by designating a different user(s) to be entitled to accessing each of a plurality of servers on an internal network which provide the same service, the security level for each server can be easily adjusted. Furthermore, in the case where the address information (LA, LP) of a server on an internal network

is altered, the present fire wall apparatus can still associate the server with the altered address information by recognizing a fixed value which identifies the server. Therefore, the alteration of tables used for address conversion can be automatically processed with ease. Moreover, the present fire wall apparatus provides a validity term for any service which can be provided to an external network, and temporarily sets a communication path only while the service is valid, and the communication path is dedicated to that service. Thus, a more enhanced level of security can be realized.

In the present embodiment, when a pair consisting of the service type and the server identification information of a service to be registered has not been registered in the directory management function section 33, detailed service permission policies are set based on basic service permission policies, as shown in step S109 of FIG. 4. Alternatively, the detailed service permission policies may be determined by other methods. For example, among the entries which are already registered in the detailed service permission policies, the number of those which are of the same service type as that of the service to be newly registered may be counted, and detailed service permission policies may be set based on the already registered entries if that number is equal to or greater than a certain threshold value; or, if the number is smaller than the threshold value, detailed service permission policies may be set based on the basic service

permission policies. In other words, the process shown in FIG. 14 may be executed in stead of step S109 shown in FIG. 4. Hereinafter, this will be described more specifically with reference to FIG. 14 to FIG. 16.

Assume, for example, that a server 2-4 whose IP is LA5 is newly introduced to the internal network. In other words, the case in which service information as shown in FIG. 15 is newly registered in the directory management function section 33. Upon determining at step S102 in FIG. 4 that a service being provided by the server 2-4 is unregistered, the directory management function section 33 at step S203 in FIG. 14 extracts entries concerning the service to be newly registered, from among the detailed service permission policies which are already managed in the directory management function section 33. Next, at step S204, the directory management function section 33 determines whether the number of extracted entries is equal to or greater than three, and if it is smaller than three, sets detailed service permission policies through a process similar to step S109 in FIG. 4. On the other hand, if it is determined at step S204 that the number of entries is equal to or greater than three, detailed service permission policies are set at step S206 based on the content of the settings of the extracted entries. This process will be described more specifically with reference to FIG. 16. With respect to the service of the type "HTTP server" on the newly-added server 2-4, two entries (i.e., entries A and B in

the following descriptions of other embodiments of the present invention.

(second embodiment)

FIG. 17 illustrates the structure of a communication apparatus 100 according to a second embodiment of the present invention. The communication apparatus 100 comprises a control menu construction section 110, a directory management function section 120, and a restriction entry management section 130. The control menu construction section 110 includes a control menu generation request reception section 111, a control menu generation section 112, and a control menu transmission section 113. The directory management function section 120 includes a network component element detection section 121, a network information acquisition section 122, and a network information storage section 123. The restriction entry management section 130 includes a restriction entry generation section 131, a preset restriction entry storage section 132, an individual restriction entry storage section 133, and an input section 134.

The communication apparatus 100 has the function of, when a user wishes to control a "controlled" terminal from a "controlling" terminal via a network, either permitting such control, partially restricting such control, or prohibiting such control, based on predetermined restriction entries. For example, a VCR (video cassette recorder) connected to a network (IEEE1394 bus) which is installed in the home of a person named

FIG. 16) are found to match this service type. Therefore, the permitted recipient, the permission condition, and the permitted port for the service of the type "HTTP server" on this server 2-4 are determined based on the basic service permission policies shown in FIG. 9. On the other hand, with respect to the service of the type "FTP server" on the server 2-4, three entries (i.e., entries C to E in FIG. 16) are found to match this service type. Therefore, the permitted recipient, the permission condition, and the permitted port for the service of the type "FTP server" on this server 2-4 are determined based on the content of the settings of entries C to E. In this case, those settings which are common to entries C to E will be reflected on the settings of the service of the type "FTP server" on the server 2-4.

As for the specific methods for setting detailed service permission policies based on the content of the settings of the extracted entries, various methods are possible. For example, although the above description illustrates that the detailed service permission policies are generated in such a manner that the content of the settings of the new service is determined based on a logical AND of the contents of the settings of the already registered entries, the present invention is not limited thereto. For example, the content of the settings of the new service may be determined based on a logical OR or on a majority among the contents of the settings of the already registered entries. These or various other setting methods will also become apparent from

"Jack" may be controlled as a "controlled" terminal via the network in the following manner. That is, the communication apparatus 100 may allow Jack to control the VCR from either a "controlling" terminal which is connected to the in-home network or from a mobile phone as a "controlling" terminal connected to the Internet, while allowing a daughter of Jack named "Jill" to control the VCR only from a "controlling" terminal which is connected to the in-home network, but not from a mobile phone. Thus, the control over the "controlled" terminal is restricted under certain conditions.

FIG. 17 shows an exemplary configuration in which "controlled" terminals 151 to 153 (e.g., VCR's or tuners) which are connected to an IEEE1394 bus 170 (as an in-home network) are controlled from a "controlling" terminal 141 (e.g., a mobile phone) which is connected to the Internet 160 (as an out-of-home network), where the controlled terminals 151 to 153 are equipped with AV/C commands.

Hereinafter, the operation of the communication apparatus 100 will be described.

The directory management function section 120 manages as element information the information concerning the devices which are connected to the network. FIG. 18 shows an example of element information which is managed by the network information storage section 123. In FIG. 18, "GUID" is a 64-bit identifier which is uniquely assigned to each device; "device category" indicates a

device type; "service information" indicates the service(s) which the device can provide to the network; and "embracing network" indicates the network to which the device belongs. Thus, the element information shown in FIG. 18 indicates that two VCR's which can be controlled over the network with respect to "power" "record", "playback", "fast forward", "rewind", and "stop", as well as a tuner which can be controlled over the network with respect to "power" and "tune", are connected as devices the IEEE1394 bus.

The directory management function section 120 has the function of detecting any new device that is connected to the network to which the communication apparatus 100 is connected, and updating the element information. Hereinafter, this function will be described with respect to a specific example. FIG. 19 illustrates an operation sequence in the case, where devices 152 and 153 are already connected to the IEEE1394 bus 170, a device 151 is newly connected to the IEEE1394 bus 170. Note that, in the following description and also in the subsequent embodiments, the controlled terminal 151 or the like in FIG. 17 will merely be referred to as a "device" 151, etc. The reason behind this is that a device which is connected to a network does not need to be predesignated to be a "controlling" or "controlled" terminal. If the device is a PC (Personal Computer) or the like, the device may be utilized as a controlling terminal or as a controlled terminal depending on the situation. Thus,

references to a "device 151" or the like will be made where the device is not yet determined to be an agent or an object of control.

A bus resetting occurs when a new device (i.e., the device 151 in this example) is connected to the IEEE1394 bus 170. The bus resetting is detected by the network component element detection section 121, which notifies the occurrence of bus resetting to the network information acquisition section 122. Upon receiving this notification, the network information acquisition section 122 acquires the GUID's of the devices which are connected to the IEEE1394 bus 170. The network information acquisition section 122 notifies the acquired GUID to the network information storage section 123.

Referring to the element information which is already stored, the network information storage section 123 compares the GUID notified from the network information acquisition section 122 against the GUID(s) of the device(s) which was connected prior to the occurrence of bus resetting. As a result, it is confirmed that the GUID of the device 151 has been added. Accordingly, in order to update the element information, the network information storage section 123 requests the network information acquisition section 122 to acquire the service information provided from the newly-connected device 151 and the device category thereof. Using an AV/C command, the network information acquisition section 122 acquires the service information provided from the device 151 and information indicating the device category

thereof.

The network information acquisition section 122 notifies the acquired service information provided from the VCR (A) 151 and the information indicating the device category thereof to the network information storage section 123. The network information storage section 123 updates the element information by registering the notified information in the element information.

In order to control a "controlled" terminal from a "controlling" terminal, a user first makes a request to the communication apparatus 100 for a control menu for controlling the controlled terminal. In response to the request from the controlling terminal, the control menu construction section 110 constructs a control menu and sends it to the controlling terminal. FIG. 20 shows an exemplary displayed image of a control menu which is sent to the controlling terminal. Based on this control menu, the user can control the controlled terminal (e.g., begin recording on the VCR (A) 151) from the controlling terminal. In the restriction entry management section 130, predetermined restriction entries which stipulate whether to permit or prohibit controlling of controlled terminals under various conditions are registered. FIG. 21 shows examples of restriction entries which are managed in the restriction entry management section 130. In the examples shown in FIG. 21, restriction information which indicates whether to permit or prohibit controlling of controlled

terminal is designated for each set of control conditions, which is defined by a combination of: a controlled terminal; a user who wishes control ability; a network to which the controlling terminal belongs; and a network which embraces the controlled terminal. In the case of FIG. 21, for any controlled terminal having a GUID "0x0123456789012345" which is connected to "IEEE1394", control is permitted to "Jack", who wishes to exert control from a controlling terminal connected to the "Internet", because "access enabled (1)" is set as the restriction information. On the other hand, for any controlled terminal having a GUID "0x0123456789012345" which is connected to "IEEE1394", control is not permitted to "Jill", who wishes to exert control from a controlling terminal connected to the "Internet", because "access disabled (0)" is set as the restriction information. To each controlling terminal, a control menu is sent which is generated based on the corresponding restriction entry managed in the restriction entry management section 130 and which only contains items that are permitted for control from the controlling terminal. Thus, control of the controlled terminal from a controlling terminal is restricted based on the corresponding restriction entry which is managed in the restriction entry management section 130.

Hereinafter, an exemplary process in which a user acquires a control menu from a controlling terminal will be specifically described. FIG. 23 illustrates an operation sequence in the case

is requested at this point comprises a device GUID, a device category, service information, and the type of the network. Based on the element information which is managed in the aforementioned manner, the network information storage section 123 notifies the element information to the control menu generation section 112.

Next, the control menu generation section 112 notifies the user ID and the network information concerning the controlling terminal received from the control menu generation request reception section 111 and the element information received from the network information storage section 123 to the restriction entry generation section 131, and requests a restriction entry corresponding to such information.

Upon receiving the restriction entry request from the control menu generation section 112, the restriction entry generation section 131 transmits the "GUID", "user ID", "network embracing the controlled terminal", "network embracing the controlling terminal", which have been notified from the control menu generation section 112, to the individual restriction entry storage section 133. The individual restriction entry storage section 133, where the aforementioned restriction entries shown in FIG. 21 are previously registered, searches for restriction information that matches the information transmitted from the restriction entry generation section 131, and notifies the matching information to the restriction entry generation section 131. For example, if the element information contains

information concerning a device whose GUID is "0x0123456789012345", then the restriction information corresponding to a combination consisting of "IEEE1394" (i.e., the network to which this device is currently connected), "Jack" (i.e., the ID of the user who wishes to control this device), and "Internet" (i.e., the network to which the controlling terminal is connected) is searched for. The result of the search in this example indicates that "access enabled (1)" is set as the restriction information. Similar searches are made with respect to devices having any other GUID's that are contained in the element information. The individual restriction entry storage section 133 notifies the restriction information thus obtained to the restriction entry generation section 131.

Note that the individual restriction entries shown in FIG. 21 include individual restriction entries for the newly-connected device 151 (shown as new entries A, B in FIG. 21) having already been registered through the below-described process and the like. On the other hand, the presently-described operation sequence is based on the assumption that such new entries A and B are yet to be registered. Therefore, the individual restriction entries which exist at this point would appear as shown in FIG. 22.

On the other hand, the search result by the individual restriction entry storage section 133 may indicate that no restriction entries which match the particular set of conditions are registered. Such a situation may occur when a new device is

connected to the network as a controlled terminal, or in some cases, when a device is connected to a different network, for example. A similar situation may also occur in the case where Jack has been registered but Jill has not been registered yet. In such situations, conventional techniques have a problem, as described earlier, in that the user needs to set restriction entries for any newly-connected device. Therefore, if a person without sufficient knowledge on network management (e.g., a member of the family) happens to connect a device to a network, unrestricted access to such items might occur from outside of the house based on improper settings.

In contrast, according to the present embodiment of the invention, if the search result by the individual restriction entry storage section 133 indicates that no restriction entries which match a particular set of conditions are registered yet, then restriction information which matches the set of conditions is acquired based on the preset restriction entries which are previously set in the preset restriction entry storage section 132. As a result, restriction information which designates preferable restrictions is automatically set, without requiring the user to perform a setting operation. More specifically, for a set of conditions which does not have any corresponding restriction entries registered, the restriction entry generation section 131 transmits the "user ID", "network embracing the controlling terminal", and the "network embracing the controlled

terminal" to the preset restriction entry storage section 132. Then, the preset restriction entry storage section 132 searches for restriction information which matches these conditions among the preset restriction entries, and notifies such restriction information to the restriction entry generation section 131. FIG. 24 shows exemplary preset restriction entries which may be registered in the preset restriction entry storage section 132. In FIG. 24, if a new device is connected to "IEEE1394" and thereafter "Jack" requests a control menu from a controlling terminal connected to the "Internet", for example, a result of the search for preset restriction entries corresponding to the above conditions would indicate that "access enabled (1)" is set as restriction information matching these conditions. Accordingly, "access enabled (1)" is notified to the restriction entry generation section 131.

Based on the restriction information notified from the preset restriction entry storage section 133, the restriction entry generation section 131 registers a new restriction entry to the individual restriction entry storage section 133. For example, if the controlled terminal 151 having the GUID "0x0123456789012345" is newly connected to the IEEE1394 bus 170 and thereafter "Jack" requests a control menu from the controlling terminal 141 which is connected to the Internet 160, "access enabled (1)" is set for the preset restriction entry which matches these conditions (that is, except for the GUID). Accordingly,

113. In turn, the control menu transmission section 113 transmits the received control menu to the controlling terminal (i.e., the controlling terminal 141 in this example). The controlling terminal 141 displays the control menu on a browser, and the user is allowed to manipulate the controlled terminals 151 to 153 based on the control menu.

Now, with reference to the flowchart of FIG. 25, the operation of the restriction entry generation section 131 will be described. For clarity, the following description will be directed to a specific exemplary case where the element information shown in FIG. 18 is stored in the network information storage section 123, and the preset restriction entries shown in FIG. 24 are stored in the preset restriction entry storage section 132, further assuming that the restriction entries concerning the controlled terminal 151 whose GUID is "0x0123456789012345" (i.e., new entries A, B in FIG. 21) among the individual restriction entries shown in FIG. 21 have not been registered (that is, only the restriction entries shown in FIG. 22 are registered).

At step S901, the restriction entry generation section 131 receives from the control menu generation section 112 the conditions based on which to generate restriction information, i.e., the "GUID", "user ID", "network embracing the controlling terminal" information, and "network embracing the controlled terminal" information. Specifically, the following entries are received at this step:

GUID = 0x0123456789012345

user ID = Jack

"network embracing the controlled terminal" information = IEEE1394 (hereinafter simply referred to as "in-home")

"network embracing the controlling terminal" information = Internet (hereinafter simply referred to as "out-of-home")

GUID = 0x0123456789123456

user ID = Jack

"network embracing the controlled terminal" information = in-home

"network embracing the controlling terminal" information = out-of-home

GUID = 0x0123456789234567

user ID = Jack

"network embracing the controlled terminal" information = in-home

"network embracing the controlling terminal" information = out-of-home

At step S902, based on the above conditions, a request for sending individual restriction entries is made to the individual restriction entry storage section 133. At step S903, the restriction information corresponding to the above conditions are received. Specifically, the following entries are received at this step:

GUID = 0x0123456789012345

user ID = Jack,

"network embracing the controlled terminal" information = in-home

"network embracing the controlling terminal" information = out-of-home

restriction information =

GUID = 0x0123456789123456

user ID = Jack

"network embracing the controlled terminal" information = in-home

"network embracing the controlling terminal" information = out-of-home

restriction information = access enabled

GUID = 0x0123456789234567

user ID = Jack,

"network embracing the controlled terminal" information = in-home

"network embracing the controlling terminal" information = out-of-home

restriction information = access enabled

At step S904, it is confirmed whether or not any set of conditions exists which does not have corresponding restriction information. If there is such a set of conditions, the control proceeds to step S905; otherwise, the control proceeds to step S908. In this example, the set of conditions beginning with GUID

= 0x0123456789012345 is a set of conditions which does not have corresponding restriction information.

At step S905, with respect to the set of conditions which does not have corresponding restriction information, a request for notifying restriction entries corresponding to this set of conditions (that is, except for the GUID and the restriction information) is made to the preset restriction entry storage section 132. At step S906, restriction information matching such conditions is received. Specifically, the following entry is received at this step:

user ID = Jack,

"network embracing the controlled terminal" information = in-home

"network embracing the controlling terminal" information = out-of-home

restriction information = access enabled

At step S907, the restriction entry received at step S906 is registered in the individual restriction entry storage section 133. As a result, an individual restriction entry (indicated as new entry A in FIG. 21) is newly registered. At step S908, an entry which associates the control conditions with restriction information is notified to the control menu generation section 112.

Thereafter, the control menu generated by the control menu generation section 112 is transmitted to the controlling terminal

141 via the control menu transmission section 113. The control menu generation section 112 generates a control menu by selecting, from the service information shown in FIG. 18, only those items for which access is permitted based on the individual restriction entries shown in FIG. 21. Thus, as shown in FIG. 20, a control menu including the VCR (A) 151, the VCR (B) 152, and the tuner 153 is displayed on the controlling terminal 141 which is manipulated by the user "Jack".

On the other hand, if the user who has requested a control menu is Jill, new entry B shown in FIG. 21 is newly registered through similar processes to those described above, and the control menu generation section 112 generates a control menu by selecting, from the service information shown in FIG. 18, only those items for which access is permitted based on the individual restriction entries shown in FIG. 21. However, since the user "Jill" is denied access via the Internet 160 with respect to all restriction entries in this example, an image as shown in FIG. 26, in which no controllable control items are displayed, is presented on the controlling terminal 141 manipulated by the user "Jill".

The individual restriction entries stored in the individual restriction entry storage section 133 can be set by the user by means of the input section 134. The individual restriction entries which are generated by the restriction entry generation section 131 and registered in the individual restriction entry storage section 133 can also be set by the user by means of the

input section 134. The preset restriction entries stored in the preset restriction entry storage section 132 can also be set by the user by means of the input section 134.

Although a request for a control menu from the controlling terminal 141 which is connected to the Internet 160 is illustrated as an example of access from outside of the home in the present embodiment, the out-of-home network may be any network other than the Internet. Moreover, a control menu may be requested from a controlling terminal connected to an in-home network, e.g., the IEEE1394 bus 170 or any other network to control a "controlled" apparatus.

Although the present embodiment illustrates "Jack" and "Jill" as user ID's, these are merely exemplary of ID's for identifying users, and may instead be set up to the discretion of each user. Although user ID's which are directed to individuals such as "Jack" and "Jill" are illustrated as a condition concerning users, the condition may instead be classified based on an attribute of users, e.g., network administrators, family members, or guests.

Although the present embodiment illustrates the IEEE1394 bus 170 as a network to which controlled terminals are connected and the Internet 160 as a network to which controlling terminals are connected, any other network may be used instead. The networks may be wired or wireless. Examples of other networks include ECHONET, Bluetooth, etc.

storage section 123. Alternatively, when the control menu generation section 112 requests element information, the network information acquisition section 122 may acquire element information, and notify it to the control menu generation section 112. In the case where element information is stored, there is an advantage in that the an improved response to user manipulation is provided. In the case where element information is acquired on demand, on the other hand, there is an advantage in that storage capacity for storing element information is unnecessary.

Although the present embodiment illustrates an example where restriction entries corresponding to new conditions are generated when generating a control menu, it is also possible to generate such restriction entries at an earlier time. For example, the generation of such restriction entries may occur upon detection of a new component element. In this case, there is an advantage in that the length of the time which lapses after a user requests a control menu until the control menu is received is reduced as compared to the case where such restriction entries are generated at the time of generating a control menu.

As described above, according to the second embodiment, even if no individual restriction entries are found that correspond to a given set of conditions, access restrictions can be realized based on preset restriction entries. Therefore, a user does not need to set access restrictions at each time. Thus, it is possible to start using any new service to be used without

having to make access settings for each service.

Since access restrictions are set based on the type of network to which a controlling device is connected, both convenience-oriented and security-oriented restrictions can be realized by, for example, permitting access with respect to a network which are open to the indefinite public (e.g., the Internet) while prohibiting access with respect to in-home networks such as IEEE1394 buses.

(third embodiment)

Hereinafter, a communication apparatus according to a third embodiment of the present invention will be described with reference to the figures.

FIG. 27 illustrates the communication apparatus 1000 according to the present embodiment, networks connected thereto, and controlling terminals and controlled terminals connected to the networks. As shown in FIG. 27, the communication apparatus 1000 includes a control menu construction section 110, a directory management function section 120, and a restriction entry management section 1030. The control menu construction section 110 includes a control menu generation request reception section 111, a control menu generation section 112, and a control menu transmission section 113. The directory management function section 120 includes a network component element detection section 121, a network information acquisition section 122, and a network information storage section 123. The restriction entry

information storage section 123. Note that the element information shown in FIG. 29 does not contain the "network embracing the controlled terminal" information shown in FIG. 18. This is because information concerning the network embracing a controlled terminal is not included as a condition in the restriction entries for setting restriction information.

As in the second embodiment, the control menu construction section 110 generates a control menu in response to a request from the controlling terminal 141. At this time, a request for restriction entries is made to the restriction entry management section 1030. The restriction entry management section 1030 returns to the control menu generation section 112 any restriction entries that correspond to a set of conditions which is notified from the control menu generation section 112. However, unlike in the second embodiment, a preset restriction entry storage section is omitted in the present embodiment. Instead, in the case where no restriction entry that matches the notified set of conditions is found in the individual restriction entry storage section 133, restriction information which designates preferable restrictions (that correspond to the set of conditions which does not have any corresponding restriction entries registered) is automatically determined based on the restriction entries which are already stored in the individual restriction entry storage section 133. Hereinafter, the details of this operation will be described.

FIG. 30 illustrates an operation sequence in the case where a user which is registered with the user ID "Jack" acquires a control menu for controlling the controlled terminal 151 using the mobile phone 141 connected to the Internet. The series of processes from requesting a control menu through manipulation of the controlling terminal 141 to the issuance of a restriction entry request to the restriction entry generation section 1031 is similar to that in the second embodiment, and the descriptions thereof are omitted.

The restriction entry generation section 1031 sends the received set of conditions to the individual restriction entry storage section 133, and requests issuance of corresponding restriction entries. The individual restriction entry storage section 133 searches for restriction information that matches the received set of conditions, and notifies the result of the search to the restriction entry generation section 1031. FIG. 31 shows examples of restriction entries which may be stored in the individual restriction entry storage section 133.

Note that the individual restriction entries shown in FIG. 31 include individual restriction entries for the newly-connected device 151 (shown as new entries A, B in FIG. 31) having already been registered through the below-described process. On the other hand, the presently-described operation sequence is based on the assumption that such new entries A and B are yet to be registered.